QUINN EMANUEL URQUHART & SULLIVAN, LLP

Diane M. Doolittle (CA Bar No. 142046)
dianedoolittle@quinnemanuel.com
Thao Thai (CA Bar No. 324672)
thaothai@quinnemanuel.com
555 Twin Dolphin Drive, 5th Floor
Redwood Shores, CA 94065
Telephone: (650) 801-5000
Facsimile: (650) 801-5100

Andrew H. Schapiro (admitted *pro hac vice*)
andrewschapiro@quinnemanuel.com
191 N. Wacker Drive, Suite 2700
Chicago, IL 60606
Telephone: (312) 705-7400
Facsimile: (312) 705-7401

Stephen A. Broome (CA Bar No. 314605)
stephenbroome@quinnemanuel.com
Viola Trebicka (CA Bar No. 269526)
violatrebicka@quinnemanuel.com
865 S. Figueroa Street, 10th Floor
Los Angeles, CA 90017
Telephone: (213) 443-3000
Facsimile: (213) 443-3100

William A. Burck (admitted *pro hac vice*)
williamburck@quinnemanuel.com
Josef Ansorge (admitted *pro hac vice*)
josefansorge@quinnemanuel.com
1300 I. Street, N.W., Suite 900
Washington, D.C. 20005
Telephone: 202-538-8000
Facsimile: 202-538-8100

Jonathan Tse (CA Bar No. 305468)
jonathantse@quinnemanuel.com
50 California Street, 22nd Floor
San Francisco, CA 94111
Telephone: (415) 875-6600
Facsimile: (415) 875-6700

Attorneys for Defendant Google LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA, SAN JOSE DIVISION

CHASOM BROWN, MARIA NGUYEN, and WILLIAM BYATT, individually and on behalf of all similarly situated,

Plaintiffs,

v.

GOOGLE LLC and ALPHABET INC.,

Defendants.

Case No. 5:20-cv-03664-LHK

DEFENDANT GOOGLE'S NOTICE OF MOTION AND MOTION TO DISMISS FIRST AMENDED COMPLAINT

The Honorable Lucy H. Koh
Courtroom 8 – 4th Floor
Date: February 25, 2021
Time: 1:30 p.m.

Amended Complaint Filed: Sept. 21, 2020

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

Please take notice that, on February 25, 2021 at 1:30 p.m. the undersigned will appear before the Honorable Lucy H. Koh of the United States District Court for the Northern District of California at the San Jose Courthouse, Courtroom 8, 4th Floor, 280 South 1st Street, San Jose, CA 95113, and will then and there present Defendant Google's Motion to Dismiss First Amended Complaint ("Motion").

The Motion is based on this Notice of Motion and Motion, the attached Memorandum of Points and Authorities, the accompanying Request for Judicial Notice, the Declaration of Andrew H. Schapiro and exhibits attached thereto, the pleadings and other papers on file in this action, any oral argument, and any other evidence that the Court may consider in hearing this Motion.

ISSUE PRESENTED

Whether the First Amended Complaint, ECF No. 68 ("AC"), along with the documents referenced and incorporated therein and judicially noticeable documents, show that Plaintiffs fail to state a claim upon which relief can be granted, thus warranting dismissal of the AC under Rule 12(b)(6).

RELIEF REQUESTED

Google requests that the Court dismiss the AC without leave to amend.

DATED: October 21, 2020

Respectfully submitted,

QUINN EMANUEL URQUHART & SULLIVAN, LLP

By */s/ Andrew H. Schapiro*
Andrew H. Schapiro
Attorneys for Defendant Google LLC

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutory Authorities

Additional Authorities

MEMORANDUM OF POINTS AND AUTHORITIES

I. PRELIMINARY STATEMENT

This case is based on a willful misreading of Google's statements about "private browsing." Plaintiffs quote partial phrases from Google's Privacy Policy and select support pages out of context to argue that Google led them to believe enabling their browsers' "private browsing" mode would prevent Google from receiving certain data generated by their browsing on websites that use Google's Analytics and Ad Manager services. But no plausible reading of the documents quoted in the First Amended Complaint ("AC") supports Plaintiffs' allegations.

Many popular browsers, including Google Chrome, offer a private browsing mode that allows users to prevent their browsing history from being stored locally on their browser. Private browsing is particularly useful for those who share devices. A user who plans to surprise her partner with a vacation, for example, may use private browsing to ensure her partner does not discover she browsed the web for "Caribbean cruises."

Plaintiffs allege Google "intercepted" data associated with their web browsing while using private browsing mode in Google's Chrome browser and Apple's Safari browser.[1] *See, e.g.*, AC ¶¶ 168, 173. Google neither controls, nor is responsible for, how private browsing works in Safari or what Apple tells its users about what private browsing means on Safari. However, private browsing typically means that (1) the private browsing session begins with a fresh cookie store, such that cookies[2] set on the browser *before* the session are not shared with the websites visited and thus the device appears as a new visitor; and (2) the user's searches, browsing history, and cookies placed on the browser *during* the private browsing session that could be used to link the user's browsing activity to them or their device, are deleted when the session is closed.

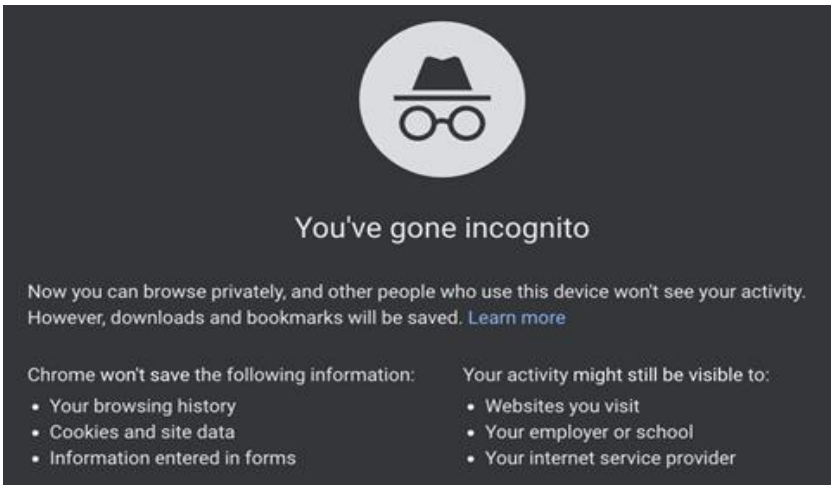
---

[1] All Plaintiffs allege that they used private browsing mode in Chrome. Only one Plaintiff, Nguyen, alleges she also used private browsing in a browser other than Chrome (Safari). AC ¶ 173.

[2] The Federal Trade Commission explains: "A cookie is information saved by your web browser. When you visit a website, the site may place a cookie on your web browser so it can recognize your device in the future. If you return to that site later on, it can read that cookie to remember you from your last visit and keep track of you over time." *See* https://www.ftc.gov/site-information/privacy-policy/internet-cookies (last accessed October 21, 2020).

Google's disclosures make clear that this is what happens when browsing in "Incognito"—Chrome's private browsing mode. Google also makes clear that "Incognito" does not mean "invisible," and that the user's activity during that session may be visible to websites they visit, and any third-party analytics or ads services the visited websites use.

This information is clearly disclosed in Google's Privacy Policy, Chrome Privacy Notice, and other notices about private browsing. Among them, as Plaintiffs acknowledge (*id.* ¶ 52), is a ***full-page*** notice (the "Incognito Notice") that appeared ***every time*** Plaintiffs opened a new Incognito window or tab, and which described the mode's practical effects in plain and concise terms:



Despite this clear disclosure that Plaintiffs indisputably reviewed multiple times, Plaintiffs selectively quote various other Google disclosures—none of which they allege they actually reviewed—to argue that Google led them to believe using private browsing mode would prevent Google from receiving certain data Google receives to provide its Analytics and Ad Manager services to third-party websites, such as "a referer header containing the URL information," "IP address," "[i]nformation identifying the browser software," "'User-ID' issued by the website," "Geolocation of the user," and "[i]nformation contained in 'Google Cookies'" (collectively, the "Data"). *Id.* ¶ 63. But Google's Privacy Policy—to which Plaintiffs consented when they signed up for their Google accounts—explains that Google receives *exactly* this Data:

> We collect information about the services that you use and how you use them, like when you … visit a website that uses our advertising services, or view or interact with our ads or content. This information includes: … details of how you used our service, such as search queries … internet protocol [IP] address… referral URL… cookies that may uniquely identify your browser… [l]ocation information … [such as] GPS.

Plaintiffs acknowledge this. They allege that "[i]t is common knowledge that Google collects information about the web-browsing activity of users who are *not* in 'private browsing mode.'" *Id.* ¶ 163 (emphasis in original). Accordingly, the only question presented here is whether Google deceived users into believing that private browsing mode would *prevent* Google from receiving the Data. It did not. Consistent with the Incognito Notice, Google's other disclosures—quoted in the AC—explain that "although [p]rivate browsing works differently depending on which browser you use," it "usually means" that "[t]he searches you do or sites you visit won't be *saved to your device or browsing history*," and cookies placed on the browser during a private browsing session "are deleted *after* you close your private browsing window or tab," (*id.* ¶ 48 (emphases added); Ex. 18) such that Data generated while users are in private browsing mode and logged out of their Google accounts (as Plaintiffs allege here, AC ¶ 192) is not correlated with (1) a particular user, browser, or device after the private browsing session is closed, or (2) Data generated during other private browsing sessions.

Plaintiffs strain to conform their allegations to the Ninth Circuit's decision in *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020), but this case is nothing like *Facebook*. Facebook allegedly (1) collected browsing history data from logged-out users despite its representation that "[i]f you log out of Facebook, *we will not receive this information*," and then (2) used cookies to "correlate[] users' browsing history *with users' personal Facebook profiles*—profiles that could include a user's employment history and political and religious affiliations [giving] Facebook [] a cradle-to-grave profile without users' consent." *Id.* at 599, 602 (emphases added). Here, in contrast, Google never represented that using private browsing would prevent Google from receiving the Data. And Plaintiffs do not plausibly allege that Google has correlated Data from private browsing sessions with them (or their accounts or devices) after they closed the sessions, or that Google has connected the Data from separate private browsing sessions. The fact that a website was visited or a search was made is not "private" information where, as here, that information is not linked to a particular user or account, and *Facebook* does not suggest otherwise.

The five claims asserted in the AC should be dismissed.[3] They fail at the outset because consent is a defense to each claim. Plaintiffs consented to Google's Privacy Policy, which disclosed that Google receives the Data to provide its Analytics and Ad Manager services. Indeed, Plaintiffs acknowledge that Google's receipt of such Data is "common knowledge." AC ¶ 163. Google's statements about private browsing generally, and Incognito in particular, did not negate that consent. To the contrary, the Incognito Notice reminded Plaintiffs *every time* they opened an Incognito window or tab that private browsing means simply that other people who use the device will not see their activity, but that activity might still be visible to third parties. The websites with which Plaintiffs allegedly "communicated" also consented, which independently defeats their claims under the Wiretap Act, a "one-party consent" statute.

Each of the claims must also be dismissed because Plaintiffs fail to plausibly allege the other elements of their claims, *see infra* § III.B, and because the claims are irredeemably time-barred, *see infra* § III.C.

II. BACKGROUND AND PLAINTIFFS' ALLEGATIONS

A. Plaintiffs Consented to Google's Privacy Policy

Plaintiffs "are Google subscribers whose internet use was [allegedly] tracked by Google" between June 1, 2016 and the present. AC ¶ 11. Although Plaintiffs allege that they have had active Google accounts and have been Gmail users for the proposed class period (beginning June 1, 2016), they omit the dates they signed up for their accounts—notwithstanding the fact that Google pointed out this deficiency in its previous motion. *See id.* ¶¶ 166-86; ECF No. 53, at 5. The reasonable inference from the AC is that Plaintiffs signed up for their accounts at some point on or before June 1, 2016. *See* AC ¶ 11. Google required users to consent to its Terms of Services ("ToS") to create

[3] Plaintiffs allege violations of: (1) the federal Wiretap Act, 18 U.S.C. §§ 2511, *et seq.*; (2) California's Invasion of Privacy Act ("CIPA"), Cal. Penal Code §§ 631 and 632, *et seq.*; (3) California's Computer Crime Law ("CCCL"), Cal. Penal Code §§ 502, *et seq.*; (4) the right to privacy under Article 1, section 1 of the California Constitution; and (5) the common law doctrine of intrusion upon seclusion.

accounts during this period.[4] Ex. 16 at 1. The ToS in effect during this period, in turn, required Plaintiffs to consent to Google's Privacy Policy. *Id.* at 3. Google's ToS effective April 14, 2014 through October 25, 2017, for example, stated that "Google's privacy policies explain how we treat your personal data and protect your privacy when you use our Services. By using our Services, you agree that Google can use such data in accordance with our privacy policies."[5] *Id.* The words "privacy policies" were blue and hyperlinked so that the user could easily navigate to them. *Id.*

B. The Privacy Policy Disclosed that Google Receives the Data

Internet users commonly provide a range of basic data to the sites they visit, which sites may use to tailor advertising that generates revenue to support their content. Plaintiffs acknowledge that "it is *common knowledge* that Google collects information about the web-browsing activity of users" and "causes targeted advertisements to be sent based on that information." AC ¶ 163 (emphasis added). Many websites use third-party services—such as Google Analytics and Ad Manager—to analyze website utilization and serve ads. To accomplish this, websites provide third-party services with information about user activity on their sites. Often they do this by installing code on their website that directs visitors' browsers to send information directly to the third-party service, as is the case with Google Analytics and Ad Manager. *Id.* ¶¶ 67-83.

The Privacy Policy and other support pages that Plaintiffs quote extensively (*id.* ¶¶ 44-50) disclosed that Google receives precisely the Data at issue in the ordinary course. The Privacy Policy in effect at the beginning of the class period (June 1, 2016), for example, stated: "We collect information about the services that you use and when you use them, like when you … visit a website that uses our advertising services, or view and interact with our ads and content." Ex. 1 at 2. The

[4] The Court can take judicial notice of Google's ToS and Privacy Policies for the reasons explained in Defendants' concurrently filed Request for Judicial Notice. In addition, the Privacy Policies and other disclosures cited in the AC are incorporated by reference.

[5] The ToS also stated: "We may modify these terms or any additional terms that apply to a Service to, for example, reflect changes to the law or changes to our Services. You should look at the terms regularly. We'll post notice of modifications to these terms on this page. We'll post notice of modified additional terms in the applicable Service." Ex. 16 at 7.

Privacy Policy specifically disclosed that Google receives each of the categories of Data at issue, including:

> [d]evice information … such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number….[;] [l]og information … [such as] details of how you used our service, such as your search queries … internet protocol [IP] address[;] device event information such as … the date and time of your request and referral URL[;] cookies that may uniquely identify your browser or your Google Account[;] [l]ocation information … [such as] IP address, GPS, and other sensors…[;] cookies and similar technologies to identify your browser or device.

Id. at 2-4. The Privacy Policy explained that Google receives the Data "when you interact with services we offer to our partners, such as advertising services or Google features that may appear on other sites," and "[o]ur Google Analytics product [that] helps businesses and site owners analyze the traffic to their websites and apps."[6] *Id.* at 4. The Privacy Policy further disclosed that Google uses the Data to "provide, maintain, protect and improve" Google's services, as well as develop new services and provide "tailored content," such as "more relevant … ads." *Id.*

The Privacy Policy also identifies an important distinction regarding when the Data is linked to a user's identity, and when it is not. Data "may be associated with your Google account"—*i.e.*, the individual's account (which is linked to a name and other information at registration)—*if* you are browsing the web while "you are signed in to Google." *Id*. On the other hand, if the user is *not* signed in to a Google account—as Plaintiffs allege here, AC ¶ 192—Google still receives the Data from its services installed on third-party websites but uses "cookies or similar technologies to identify your browser or device." Ex. 1 at 4. Google's private browsing disclosures explain, however, that cookies placed during a private browsing session in Chrome Incognito (and typically in other browsers) are deleted when the session is closed. *See, e.g.*, Ex. 17 at 8; Ex. 19; Ex. 27 at 9.

[6] Earlier and subsequent versions of Google's Privacy Policy contained identical or substantively identical disclosures. *See* Exs. 1-15. These Privacy Policies apply "to all of the services offered by Google Inc. and its affiliates, including YouTube, services Google provides on Android devices, and services offered on other sites (such as our advertising services)"—*e.g.*, Google Analytics and Google Ad Manager. Exs. 1-5; *see also* Exs. 6-15 (containing substantially similar disclosures).

C. Google's Disclosures Do Not Suggest Private Browsing Prevents Google from Receiving the Data from Services like Analytics or Ad Manager

Plaintiffs allege that Google led them to believe using private browsing mode would prevent Google from receiving the Data. AC ¶ 41. Plaintiffs' alleged belief is purportedly based on the Privacy Policy and other support pages quoted in the AC. *Id.* ¶¶ 44-59. Even if Plaintiffs had reviewed these documents—and they do not allege that they did—the documents do not support Plaintiffs' alleged interpretation.

For example, Plaintiffs include a screenshot of a "Search & browse privately" page, which states generally that users are "in control of what information you share with Google when you search." *Id.* ¶ 48 (screenshot); Ex. 18. The next sentence lists several options: "[Y]ou can use private browsing, sign out of your account, change your custom settings, or delete past activity." AC ¶ 48. The page specifically explains "How private browsing works" generally, and states that, although "[p]rivate browsing works differently depending on which browser you use," it "usually means" that "[t]he searches you do or sites you visit won't be *saved to your device or browsing history*." *Id.* (emphasis added). The page further explains that "cookies" placed on the browser during a private browsing session—*e.g.*, by third-party websites, Google Analytics, or Google Ad Manager—"are deleted *after* you close your private browsing window or tab." *Id.* (emphasis added). Thus, although "[y]ou might see search results and suggestions based on … other searches you've done *during* your current [private] browsing session," the cookies linking those searches to the browser or device are "deleted *after* you close your private browsing window or tab." *Id.* (emphasis added). The page also makes clear that private browsing activity and searches are not associated with an individual user or their account *unless* "you sign in to your Google Account" during the private browsing session, which Plaintiffs allege they did not do. *Id.*; *see id.* ¶ 192.

Google has multiple other, clear disclosures explaining what private browsing means—and what it does not. The "Search & browse privately" page that Plaintiffs quote links to a page titled "How private browsing works in Chrome," which similarly explains: (1) "When you browse privately, *other people who use the device* won't see your history"; and (2) "Cookies and site data are *remembered while you're browsing*, but *deleted when you exit Incognito mode*." Ex. 19

(emphases added). Google informs users that although "Incognito mode stops Chrome from saving your browsing activity *to your local history*[, y]our activity … might still be visible to: … Websites you visit, ***including the ads and resources used on those sites*** [*e.g.*, Analytics and Ad Manager]"; "Websites you sign in to"; "Your internet service provider"; and "Search Engines."[7] *Id*. (emphasis added). And the page explains that, even in private browsing, "[a] ***web service***, website, search engine, or provider may be able to see" "[y]our activity when you use a web service" and "[y]our IP address, which can be used to identify your general location." *Id*. Similarly, if a user clicks on the hyperlinked "Chrome" in the "Search & browse privately" page that Plaintiffs quote, the "Browse in private" page appears and describes "[w]hat happens when you browse privately," including that "Chrome won't save your browsing history, cookies and site data, or information entered in forms," and also makes clear that even when browsing privately, "[y]our activity isn't hidden from websites you visit, your employer or school, or your internet service provider." Ex. 20.

Google's Privacy Policies also link to Google's Chrome Privacy Notice, which similarly explains Incognito mode:

> You can limit the information *Chrome* stores *on your system* by using incognito mode or guest mode. In these modes, *Chrome* won't *store* certain information, such as: [] Basic browsing history information like URLs, cached page text, or IP addresses of pages liked from the websites you visit [and] Snapshots of pages that you visit.
>
> How Chrome handles your incognito or guest information[:]
>
> **Cookies.** Chrome won't share existing cookies with sites you visit in incognito or guest mode. Sites may deposit new cookies on your system while you are in these modes, *but they'll only be stored and transmitted until you close the incognito or guest window*.

See Ex. 17 at 7-8 (emphases added). In addition, *every time* a Chrome user opens an Incognito window or tab, the full-page Incognito Notice excerpted above on page 2 is displayed. AC ¶ 52.

---

[7] The screenshot at AC ¶ 86 does not demonstrate an inconsistency between Google's disclosures and practices. Plaintiffs are correct that Google Analytics and Ad Manager may receive data while the user is in private browsing mode; and whether data is being sent can be seen by users by using Chrome's <Developer Tool> function. As the disclosures explain, the cookies to which that data is linked are deleted when the user closes out of their private browsing session. Plaintiffs do not allege that Google's cookies persisted on their browsers after they closed a private browsing session.

In sum, Google's disclosures consistently stated that, in private browsing/Incognito mode: (1) "*other people who use this device* won't see your activity," (2) "*Chrome won't save*" the Data because, although "[c]ookies and site data are *remembered while you're browsing*, [they are] deleted *when you exit Incognito mode*," but (3) "[y]our activity might still be visible to," among others, "[w]ebsites you visit, *including the ads and resources used on those sites*." AC ¶ 52; Ex. 19 (emphases added). Google's disclosures do *not* state or suggest that private browsing/Incognito mode prevents Google from receiving the Data through its services installed on third-party websites, such as Analytics or Ad Manager.

D. Websites Choose to Embed Google's Analytics and Ad Manager Code to Allow Google to Receive Information Used to Provide Its Services

It is undisputed that websites choosing to use Google's Analytics or Ad Manager services install Google's code in their website for the purpose of transmitting the Data to Google so that Google can provide the desired services. *See* AC ¶¶ 63-68, 78-83. Plaintiffs allege, for example, that websites choose to "embed Google's own custom [Analytics] code into their existing webpage code" so Google can receive the Data to provide the websites "data analytics and attribution about the origins of a [w]ebsite's traffic, demographics, frequency, browsing habits on the [w]ebsite, and other data about visitors." *Id.* ¶ 67. Plaintiffs similarly allege that websites "embed" Google's Ad Manager code "into the [w]ebsite's code" so Google can receive Data "to display targeted Google advertisements [to display on the website] along with the [w]ebsite's actual content." *Id.* ¶ 79; *see also* Exs. 24, 25.

III. ARGUMENT

A. All Claims Should Be Dismissed Because Plaintiffs and the Websites Consented to Google's Receipt of the Data

Plaintiffs allege that Google "intercepted" their "communications" with the websites they visited in private browsing mode. *Id.* ¶ 209. But consent is a defense to each of their claims,[8] and

[8] *See* 18 U.S.C. § 2511(2)(d) (Wiretap Act) (it is not "unlawful … for a person … to intercept a[n] … electronic communication … where *one* of the parties to the communication has given prior consent to such interception") (emphasis added); Cal. Pen. Code §§ 631(a), 632(a) (CIPA)

Plaintiffs and the websites consented to Google's receipt of the alleged "communications." Indeed, only one party's consent is necessary to bar their claim under the Wiretap Act (*see* 18 U.S.C. § 2511(2)(d)) and the websites' consent cannot genuinely be disputed here.

1. Plaintiffs Consented to Google's Receipt of the Data

Plaintiffs allege that they have been Google account holders since June 1, 2016. AC ¶¶ 11-16. Therefore, they consented to Google's Terms of Service and Privacy Policy. *See supra* § II.A. The Privacy Policy specifically disclosed that Google would receive the Data, including through Analytics and Ad Manager. *See supra* § II.B; *see also Smith v. Facebook, Inc.*, 745 F. App'x 8, 9 (9th Cir. 2018) (consent established for Wiretap Act and other claims given that "Terms and Policies contain numerous disclosures related to information collection on third-party websites"); *Garcia v. Enterprise Holdings, Inc.*, 78 F. Supp. 3d 1125, 1135-37 (N.D. Cal. 2015) (dismissing CIPA claim where app provider's terms and privacy policy provided consent for the alleged disclosures).

Plaintiffs' contention that, based on certain cherry-picked Google statements about private browsing, they believed they had *withdrawn* their consent by using private browsing, is meritless. As explained in Section II.C, *supra*, Google's disclosures about private browsing generally, and Incognito mode in particular—including the conspicuous full-screen Incognito Notice shown to Plaintiffs *every time* they opened an Incognito window or tab—made clear that private browsing means: (1) "*other people who use this device* won't see your activity," (2) "*Chrome won't save*" the Data because, although "[c]ookies and site data are *remembered while you're browsing*, [they are] deleted *when you exit Incognito mode*," but (3) "[y]our activity might still be visible to," *inter alia*, "Websites you visit, *including the ads and resources on those sites*." *See* AC ¶ 52; 19 (emphases added).

(prohibiting wiretapping and eavesdropping "without the consent of all parties to the communication"); Cal. Pen. Code § 502(c)(2) (CCCL) (person who "knowingly accesses and *without permission* takes, copies, or makes use of any data" is guilty of a public offense) (emphasis added); *Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 955-56 (N.D. Cal. 2017), *aff'd*, 745 F. App'x 8 (9th Cir. 2018) ("Plaintiff's consent [] bars their common-law tort claims and their claim for invasion of privacy under the California Constitution.") (citing Cal. Civ. Code § 3515 ("He who consents to an act is not wronged by it.")).

There is no Google representation stating—or even suggesting—that private browsing would prevent Google from receiving the Data that the Privacy Policy disclosed Google ordinarily receives to perform its Analytics and Ad Manager services. Accordingly, any argument by Plaintiffs that they believed they had withdrawn consent by using private browsing is unavailing. The disclosures upon which Plaintiffs' purported belief was based do not support their interpretation.

That Plaintiffs consented to Google's receipt of the Data should be the end of the inquiry. All of their claims fail.

2. The Websites Consented to Google's Receipt of the Data

Plaintiff's Wiretap Act claim (Count 1) fails for an independent consent-based reason: the Wiretap Act is a "one-party consent" statute, and "it is not unlawful under the Act for a person to 'intercept … [an] electronic communication … where one of the parties to the communication has given prior consent to such interception.'" *In re Nickelodeon Consumer Privacy Litig.*, 2014 WL 3012873, at *13 (D.N.J. July 2, 2014) (quoting 18 U.S.C. §§ 2511(2)(d)). Because the communications at issue were shared with the consent of websites using Google's services, Plaintiffs' Wiretap Act claim should be dismissed. *See id.*

Plaintiffs allege that the websites "embedded" Google's Analytics and/or Ad Manager code into their own code to transmit the Data to Google so that Google could provide its Analytics and Ad Manager services. AC ¶¶ 64-68 (Google Analytics); *id.* ¶¶ 78-79 (Google Ad Manager). Courts have long recognized that websites that install Google's code to obtain services consent to Google's receipt of Data used to provide those services. In *In re Doubleclick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 503, 510 (S.D.N.Y. 2001), for example, the court held that websites that used DoubleClick (n.k.a. Ad Manager, AC ¶ 78) to display ads had "consented" to DoubleClick's alleged "interception" of Data generated by user interactions with those websites—including "searches performed on the Internet [and] [w]eb pages or sites visited." In granting DoubleClick's Rule 12(b)(6) motion to dismiss, the court explained that it is "implausible to infer that the Web sites have not authorized DoubleClick's access" given that:

> Doubleclick-affiliated Web sites actively notify DoubleClick each time a plaintiff sends them an electronic communication (whether through a page request, search, or

> GIF tag). The data in these notifications (such as the name of the Web site requested) often play an important role in determining which advertisements are presented to users. Plaintiffs have offered no explanation as to how, in anything other than a purely theoretical sense, the DoubleClick-affiliated Web sites could have played such a central role in the information collection and not have authorized DoubleClick's access.

154 F. Supp. 2d at 510-11; *see also Chance v. Ave. A, Inc.*, 165 F. Supp. 2d 1153, 1162 (W.D. Wash. 2001) ("It is implicit in the web pages' code instructing the user's computer to contact [defendant], either directly or via DoubleClick's server, that the web pages have consented to [defendant's] interception of the communication between them and the individual user.").

Plaintiffs' conclusory allegation, made "[o]n information and belief, [that] Google never receives consent from [w]ebsites implementing Google Analytics or otherwise that Google may continue to intercept user activity and user data … when 'private browsing mode' has been enabled" (AC ¶¶ 75, 215), is both irrelevant and implausible. It is irrelevant because such specific consent is not required. As demonstrated above, it is clear that the websites consented to Google's receipt of the Data *generally*, so that they may obtain Google's services. Nothing in Google's disclosures regarding Analytics states or suggests that a user's browser mode affects Analytics' receipt of the Data (*see* Exs. 21, 22, 23, 26), and Plaintiffs do not allege otherwise. Thus, even if "officers of certain Web sites might not understand precisely how DoubleClick collects demographic information … that knowledge is irrelevant to the authorization at issue. All that the Web sites must authorize is that DoubleClick access plaintiffs' communications to them." *In re Doubleclick Inc. Privacy Litig.*, 154 F. Supp. 2d at 510.

In addition, Plaintiffs' allegation that websites using Google's Analytics and Ad Manager services expected that Google would not receive such Data—and therefore would not be able to provide its services—for users visiting their sites in private browsing mode is entirely implausible. By Plaintiffs' flawed logic, for users in private browsing mode that access a website that uses Ad Manager, Google would not receive such basic information as IP address or device information, frustrating Google's ability to display ads, which many sites rely on for revenue to support their free content. Google plainly did not present private browsing mode as a tool to block ads. Nor did Google

present private browsing mode—to Plaintiffs, the websites, or anyone else—as a mode that would prevent the operation of Analytics or Ad Manager.

In short, Plaintiffs allege that the websites *chose* to install Google's code to transmit the Data to Google. Accordingly, the websites necessarily consented to Google's receipt of the Data—regardless of a particular user's browser choice. Therefore, even if Plaintiffs had not consented to Google's receipt of the Data from websites they visited—which they did—the Wiretap Act claim fails based on the websites' consent alone.

B. Plaintiffs' Claims Should Be Dismissed for Additional Reasons

1. Plaintiffs' Wiretap Act Claim (Count 1) Fails Because Google Received the Data in the Ordinary Course of Business

The Wiretap Act prohibits the interception of electronic communications through an "electronic, mechanical, or other device." 18 U.S.C. § 2511(1). Section 2510(5)(a) exempts from the definition of "device" any device that is "being used by a provider of wire or electronic communication service in the ordinary course of its business." *Id.* § 2510(5)(a)(ii). This Court has explained that this exception requires a "nexus between the need to engage in the alleged interception and … the ability to provide the underlying service or good." *In re Google, Inc.*, 2013 WL 5423918, at *11 (N.D. Cal. Sept. 26, 2013) (Koh, J.). That nexus is present here.

Plaintiffs allege that Google received the Data through Analytics and Ad Manager "code" that the websites "embed … into their existing webpage code." AC ¶¶ 65-79. Plaintiffs further allege that this "code" causes the Data "to be sent to Google's servers." *Id.*; *see also id.* ¶ 64 (alleging that the "secret transmission" of Data "is initiated by Google code" on the websites); *id.* ¶ 65 ("Google's embedded Google code … sends secret instructions back to the user's browser" that "cause the user's browser to secretly duplicate the communication with the website, transmitting it to Google servers in California."). Therefore, the "device" that allegedly transmits the Data to Google is the Analytics and Ad Manager code installed on the websites.

The "underlying service or good" (*see In re Google*, 2013 WL 5423918, at *11) in this case is analytics and ad services. Plaintiffs allege the Ad Manager code "causes *the user's browser to display targeted Google advertisements*." *Id.* ¶ 79 (emphasis added). Plaintiffs similarly allege that

Google's Analytics code is used to "provide[] data analytics and attribution about the origins of a Website's traffic, demographics, frequency, browsing habits on the [w]ebsite, and other data about visitors." *Id.* ¶ 67. Plaintiffs do not (and could not) allege that Google could provide Analytics or Ad Manager services *without* receiving the Data.[9]

Plaintiffs try to plead around the ordinary course of business exception by arguing that "Google, in its conduct allege here, was not providing an '[ECS],' as that term is defined in 18 U.S.C. § 2510(12)"[10] because "the conduct alleged here does not arise from Google's separate Gmail business of email communications or Google's separate GChat business of instant messages." AC ¶ 211. But the statute's definition of ECS is not limited to email or instant messaging services. Rather, it includes "any service which provides to users thereof the ability to send or receive … electronic communications."[11] 18 U.S.C. § 2510(15). "Electronic communications" include "any transfer of … data … of any nature transmitted in whole or part by a wire." *Id.* § 2510(12). On the facts alleged, Google's Analytics code and Ad Manager code—which the websites allegedly used to communicate Data to Google—fall within these definitions.

Accordingly, the ordinary course of business exception applies and Plaintiffs' Wiretap Act claim should be dismissed.

2. Plaintiffs' CIPA § 632 Claim (Count 2) Fails Because the Data Is Not a "Confidential Communication"

A separate requirement under CIPA § 632 is the existence of a "confidential communication." *In re Google*, 2013 WL 5423918, at *22. A communication is "confidential" for

---

[9] For this reason, Plaintiffs' allegations are materially distinguishable from those in *In re Google Inc.*, where this Court held that the ordinary course of business exception did not apply to Google's alleged "reading of [Gmail] user's emails" for the purpose of "creat[ing] user profiles and to provide targeted advertising" because "Google's interceptions are for Google's own benefit in other Google services unrelated to the service of email or the particular user." 2013 WL 5423918, at *8, *11 (internal quotation marks and citation omitted).

[10] Plaintiffs' reference to § 2510(12) appear to be in error. Section 2510(12) defines "electronic communication." Section 2510(15) defines "electronic communication service."

[11] Courts have held, in analogous context, that websites that use DoubleClick (k.n.a. as Ad Manager) are "users" of an ECS within the meaning of the ECPA. *See DoubleClick*, 154 F. Supp. 2d at 509.

purposes of § 632 only if a party "has an objectively reasonable expectation that the conversation is not being overheard or recorded." *Flanagan v. Flanagan*, 27 Cal. 4th 766, 768 (2002); *see also* Cal. Penal Code § 632(c). Plaintiffs fail to allege such an objectively reasonable expectation here.

"California appeals courts have generally found that Internet-based communications are not 'confidential' within the meaning of section 632, because such communications can easily be shared by … the recipient(s) of the communications." *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 849 (N.D. Cal. 2014) (dismissing § 632 claim because Facebook messenger messages are not "confidential communications); *People v. Nakai*, 183 Cal. App. 4th 499, 518-19 (2010) (criminal defendant's intent to keep his internet chats confidential did not satisfy § 632(a) because it was reasonable to assume that the communications could be recorded or shared by the service provider); *In re Google*, 2013 WL 5423918, at *22 ("Some decisions from the California appellate courts ... suggest that internet-based communication cannot be confidential [because] individuals cannot have a reasonable expectation that their online communications will not be recorded.").

Because Plaintiffs' internet-based communications are not "confidential communications," their CIPA § 632 claim should be dismissed. *See Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, at *3 (N.D. Cal. Oct. 23, 2019) (dismissing § 632 claim because "browsing activity and form field entries" are not "confidential communications"); *Cline v. Reetz-Laiolo*, 329 F. Supp. 3d 1000, 1051-52 (N.D. Cal. 2018) (dismissing § 632 claim because even "emails and other electronic messages … concern[ing] private medical and financial information" are not "considered 'confidential' under CIPA") (quotation marks omitted).

3. Plaintiffs' CCCL Claim (Count 3) Fails Because Google Did Not Take, Copy, or Make Use of the Data "Without Permission"

Plaintiffs' claim under the California Computer Crime Law ("CCCL"), Penal Code § 502(c)(2), also fails.[12] This provision applies only to one who "[k]nowingly accesses and *without permission* takes, copies, or makes use of any data from a computer, computer system, or computer network...." Cal. Penal Code § 502(c)(2) (emphasis added). Because the statute has both criminal

[12] The CCCL is also referred to as the California Computer Data Access and Fraud Act ("CDAFA").

and civil applications, it must be interpreted consistently in both contexts. *Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004). In the Ninth Circuit, to avoid being held unconstitutionally vague, a criminal statute must "(1) define the offense with sufficient definiteness that ordinary people can understand what conduct is prohibited; and (2) establish standards to permit police to enforce the law in a non-arbitrary, non-discriminatory manner." *United States v. Sutcliffe*, 505 F.3d 944, 953 (9th Cir. 2007) (internal quotation marks and citation omitted).

Courts in this District have held that liability under Section 502(c)(2) cannot attach based solely on an allegation that a defendant violated a contractual term of use because that would result in criminal liability potentially turning on issues of contract interpretation and be inconsistent with the principles articulated in *Sutcliffe*. *See Facebook, Inc. v. Power Ventures, Inc.*, 2010 WL 3291750, at *11 (N.D. Cal. July 20, 2010) (a defendant "does not access or use a computer, computer network, or website without permission simply because that [defendant] violated a contractual term of use."). Rather, "to allege that a defendant acted without permission under the CCCL, a plaintiff must allege that the offending software was designed in such a way to render ineffective any barriers the Plaintiffs must wish to use to prevent access to their information." *Brodsky v. Apple Inc.*, 2019 WL 4141936, at *9 (N.D. Cal. Aug. 30, 2019) (Koh, J.) (internal quotation marks and citation omitted); *see also NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 938, 950 (N.D. Cal. 2014) (parties act without permission when they "circumvent[ ] technical or code-based barriers") (alteration in original). As the court reasoned in *Facebook v. Power Ventures*, "[t]here can be no ambiguity or mistake as to whether access has been authorized when one encounters a technical block, and thus there is no potential failure of notice to the [defendant] as to what conduct may be subject to criminal liability, as when a violation of terms of use is the sole basis for liability." 2010 WL 3291750, at *12.

Plaintiffs fail to plausibly allege that Google's Analytics and Ad Manager code circumvented any technical or code-based barrier for Google to receive the Data when users are in private browsing mode. The Ninth Circuit has found this element satisfied where the defendant continued to access a website after the plaintiff sent a cease and desist letter and instituted an IP

block in an effort to prevent the defendant from accessing the site, which the defendant circumvented by switching IP addresses, *Facebook Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1069 (9th Cir. 2016), and where the defendant obtained the plaintiff's login credentials and acquired (and then misused) the plaintiff's information, *United States v. Christensen*, 828 F.3d 763, 783, 789 (9th Cir. 2015). There is no equivalent allegation here. Plaintiffs' bald assertion that private browsing mode is itself a "barrier" through which they sought to prevent access to the Data (AC ¶ 66), is meritless because (1) Google's Privacy Policy and other statements about private browsing do not characterize private browsing as such a "barrier," *see supra* § II.C, and (2) even if Google had characterized private browsing in that manner, Plaintiffs still would allege no more than a mere violation of alleged "terms of use," which is insufficient to establish § 502(c)(2) liability. *Facebook*, 2010 WL 3291750, at *11.

Moreover, Plaintiffs understood—and were plainly on notice—that, even in private browsing mode, their activity on third-party websites would be visible to the websites they visited. Indeed, in Chrome, the full page Incognito Notice shown to Plaintiffs every time they opened an Incognito window expressly stated that "[y]our activity might still be visible to … Websites you visit." AC ¶ 52. And Google made clear this "includ[es] the ads and resources used on those sites." Ex. 19. The fact that websites installed Google's code in order to share the Data with Google does not establish that Google did anything at all, let alone that it acted "without permission" or overcame a "barrier" to access the Data. Accordingly, Plaintiffs' CCCL claim should be dismissed. *See Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 119 (N.D. Cal. 2020) (Koh, J.) (dismissing CCCL claim because Plaintiffs failed to allege how they attempted to prevent access to their information).

4. Plaintiffs' Claims For Invasion of Privacy (Count 4) and Intrusion Upon Seclusion (Count 5) Fail Because Plaintiffs Have Not Alleged The Elements

"To state a claim for intrusion upon seclusion under California common law, a plaintiff must plead that (1) a defendant 'intentionally intrude[d] into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy[,]' and (2) the intrusion 'occur[red] in a manner highly offensive to a reasonable person.'" *Facebook*, 956 F.3d at 601 (quoting *Hernandez v.*

Hillsides, Inc., 47 Cal. 4th 272, 286 (2009)) (alterations in original). "A claim for invasion of privacy under the California Constitution involves similar elements. Plaintiffs must show that (1) they possess a legally protected privacy interest, (2) they maintain a reasonable expectation of privacy, and (3) the intrusion is 'so serious … as to constitute an egregious breach of the social norms' such that the breach is 'highly offensive.'" *Id.* (quoting *Hernandez*, 47 Cal. 4th at 287). "Because of the similarity of the tests, courts consider the claims together and ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive." *Id.* The AC fails to satisfy either element.

(a) Plaintiffs Fail to Allege a Reasonable Expectation of Privacy

Plaintiffs fail to allege a reasonable expectation of privacy in the Data, under the circumstances, for two reasons: (1) Plaintiffs consented to Google's receipt of the Data; and (2) Plaintiffs do not plausibly allege that Google correlated the Data with them or with Data from their other Incognito sessions.

First, Plaintiffs' constitutional and common law privacy claims fail at the outset, because Plaintiffs consented to Google's receipt of the Data, as explained above. *See supra* §§ II, III.A.1; *see also Smith*, 262 F. Supp. 3d at 955-56; *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1037-38 (N.D. Cal. 2014) (Koh, J.) (plaintiff asserting a privacy claim under the California Constitution "must have conducted himself or herself in a manner consistent with an actual expectation of privacy, i.e., he or she must not have manifested by his or her conduct a voluntary consent to the invasive actions of defendant") (quoting *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 26 (1994)); *In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d 767, 792 (N.D. Cal. 2019) (dismissing sub-set of intrusion upon seclusion claims when disclosures could not "be interpreted as misleading users into believing that they merely needed to adjust their privacy settings to 'friends only' to protect their sensitive information from being disseminated").

Plaintiffs make a futile attempt to tailor their claims to comport with the Ninth Circuit's decision in *Facebook*, where the Court held that users adequately alleged a reasonable expectation of privacy in their browsing history vis-à-vis Facebook while they were logged out of Facebook due

to Facebook's representations. 956 F.3d at 603-04. But the claims here are a far cry from those at issue in *Facebook*. Facebook expressly represented that "[i]f you log out of Facebook, *we will not receive this information [i.e., browsing history]*." *Id.* at 602 (emphasis added). Relying on "Facebook's affirmative statements that it *would not receive information* from third-party websites after users had logged out," the Ninth Circuit held that "Plaintiffs have plausibly alleged that Facebook set an expectation that logged-out user data would not be collected," creating a reasonable expectation of privacy that Facebook violated when it "collected [the data] anyway." *Id.* at 602, 603 (emphasis added). Here, in stark contrast, Google did not tell users that it would not receive the Data when users are logged-out and in private browsing mode, and accordingly, Google did not set an expectation that the Data would not be collected.

Second, although Plaintiffs conclusorily allege that Google "associates th[e] [D]ata with the user's 'Google profile' across its services,"[13] AC ¶¶ 54, 148, there is no coherent allegation explaining how Google is supposed to have accomplished this. In *Facebook*, plaintiffs alleged that Facebook "compiled the referer headers it collected into personal user profiles using 'cookies'—small text files stored on the user's device," that persisted after they had logged out of Facebook. 956 F.3d at 596. Plaintiffs do not and cannot make a similar allegation here. Rather, Google made clear that in private browsing mode: (1) cookies set on the user's browser *before* the private browsing session are not shared with the websites visited during that session, and thus the device appears to websites and third party services on those sites, such as Analytics or Ad Manager, as a new user/device; (2) new cookies placed on the browser *during* a private browsing session are deleted when the private browsing sessions are closed; and therefore (3) the Data from a logged-out user's private browsing session is not associated with their name, account, or device after the session is closed, or with Data generated by previous or subsequent Incognito sessions. *See* Exs. 1, 17, 19.

Plaintiffs do not and cannot allege that cookies placed during a private browsing session remain on the browser when the session is closed. Instead, Plaintiffs attempt to overcome this hurdle by alleging "on information and belief" that Google uses "the X-client-Data-Header" to "track"

---

[13] The AC does not explain what Plaintiffs mean by "Google profile."

Chrome users while they are in Incognito mode. *See, e.g.*, AC ¶¶ 178, 183, 188. Yet Plaintiffs acknowledge that the X-client-Data-Header ***is not sent*** "when the user is in Incognito mode" (*id.* ¶ 96)—*i.e.*, the only Chrome browsing mode alleged here. *See Kennedy v. Bank of America, N.A.*, 2012 WL 1458196, at *4 (N.D. Cal. Apr. 26, 2012) ("on a motion to dismiss, the court need not accept allegations that are contradicted by other allegations in the complaint or by the documents attached thereto").[14]

Plaintiffs also implausibly allege that Google uses a "unique" User-ID generated by a particular website to "track [users] *across the web*," "even when they are in 'private browsing mode'" and logged out of their Google accounts. AC ¶ 69 (emphasis added). This notion is facially implausible, and Plaintiffs do not explain how this would occur.[15] Plaintiffs also speculate that Google "accomplishes its surreptitious interception and data collection" through "fingerprinting" techniques. *Id.* ¶¶ 8, 100-04. But Plaintiffs (appropriately) stop short of alleging that Google uses "fingerprinting" to correlate Data from Incognito sessions with specific users (Google does not).

Simply put, Plaintiffs' consent to Google's receipt of the Data defeats their common law privacy claims. And, even if that were not the case, web browsing session data that is not associated with a particular user or their device after the session is closed, cannot support their privacy claims. *See, e.g.*, *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (Koh, J.) (allegation that "browsing history" shared with third parties could be "de-anonymize[d]" insufficient to state invasion of privacy claim where plaintiffs did not allege "that anyone has actually done so").

[14] Plaintiffs also do not and could not allege that Google receives the header when users browse the web in private browsing mode in a browser other than Chrome.

[15] Plaintiffs' allegation that the "User-ID" is sent from their browsers to Google (AC ¶ 63), is inconsistent with their allegation that the *websites* send the "User-ID" to Analytics (*id.* ¶ 69). There can be no claim that Google "intercepted" the "User-ID" when it is sent directly from the websites to Google. Nor can there be a claim that Google improperly accessed the "User-ID" on Plaintiffs' computers if the "User-ID" is not stored on their computers, and instead stored on websites' servers.

(b) Plaintiffs Fail to Allege a Highly Offensive Invasion of Privacy That Constitutes an Egregious Breach of Social Norms

The "California Constitution and the common law set a high bar for an intrusion to be actionable." *In re Google Assistant Privacy Litig.*, 2020 WL 2219022, at *19 (N.D. Cal. May 6, 2020) (citation and quotation marks omitted). "Many courts have found that the collection—and even disclosure to certain third parties—of personal information about the users of a technology may not constitute a sufficiently 'egregious breach of social norms' to make out a common law or constitutional privacy claim." *Id.* (collecting cases); *see also In re Google, Inc. Privacy Policy Litig.*, 58 F. Supp. 3d 968, 985 (N.D. Cal. 2014) ("Courts in this district have consistently refused to characterize the disclosure of common, basic digital information to third parties as serious or egregious violations of social norms."). Plaintiffs have failed to adequately allege any invasion of privacy, let alone one so "highly offensive" as to constitute an "egregious breach of social norms."

First, courts in this district have held that disclosure of browsing history or other personal data divorced from a specific individual does not constitute "a serious invasion of a privacy interest." In *Low*, for example, this Court held that the fact that the defendant allegedly "disclosed to third parties [the plaintiff users'] LinkedIn ID and URL of the LinkedIn profile page that the user[s] viewed (which in the aggregate disclosed users' browsing history among LinkedIn profiles)" did not constitute a "serious invasion of privacy" because "[a]lthough [p]laintiffs postulate[d] that these third parties could, through inferences, de-anonymize this data, it was not clear that anyone had actually done so." 900 F. Supp. 2d at 1025. A multitude of cases are in accord. *See, e.g.*, *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (Koh, J.) ("disclos[ure] to third parties [of] … the unique device identifier number, personal data, and geolocation information from Plaintiffs' iDevices … does not constitute an egregious breach of social norms") (citing *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (2d Dist. 2011)); *Moreno v. San Francisco Bay Area Rapid Transit Dist.*, 2017 WL 6387764, at *8 (N.D. Cal. Dec. 14, 2017) ("In this age of mobile technology the Court cannot conclude that a reasonable user would consider it highly offensive or egregious that a voluntarily downloaded mobile application which utilizes the user's cell phone

identifier and location data when the app is in use, also 'periodically' accesses that anonymous data while the application is not in use.").[16] Indeed, "courts have characterized the collection and disclosure of browsing data as 'routine commercial behavior.'" *In re Google Assistant Privacy Litig.*, 2020 WL 2219022, at *19 (distinguishing "allegations that Defendants recorded their private conversations without authorization" from "browsing history" for purposes of invasion of privacy claim).

Second, Google's receipt of the Data was "common knowledge" (AC ¶ 163) and served a legitimate commercial purpose. Plaintiffs conclusorily allege Google collected the Data "with the intent to intrude upon users' seclusion and invade their constitutional privacy." *Id.* ¶ 161 (emphasis omitted). But Courts have long understood that web services, such as Google Analytics and Ad Manager, "can serve legitimate commercial purposes." *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 294 (3d Cir. 2016); *id.* at 294-95 ("Google used third-party cookies on Nick.com in the same way that it deploys cookies on myriad others websites. Its decision to do so here does not strike us as sufficiently offensive, standing alone, to survive a motion to dismiss."); *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d at 519 ("DoubleClick's purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money by providing a valued service to commercial Web sites."). And while a routine data collection "may be highly offensive if a defendant disregards consumers' privacy choices while simultaneously 'h[olding] itself out as respecting' them," *In re Vizio, Inc., Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1233 (C.D. Cal. 2017) (citation omitted), Plaintiffs have failed to plausibly allege such circumstances here.

---

[16] *See also e.g., Yunker v. Pandora Media, Inc.*, 2013 WL 1282980, at *15 (N.D. Cal. Mar. 26, 2013) (finding the allegation that "Pandora obtained [plaintiff's] PII and provided that information to [third parties] for marketing purposes" not egregious); *Gonzales v. Uber Techs., Inc.*, 305 F. Supp. 3d 1078, 1092-93 (N.D. Cal. 2018) ("Plaintiff consented to the sharing of his geolocation data with perfect strangers (Lyft riders); thus, under the circumstances he did not have a reasonable expectation of privacy in such information."); *Belluomini v. Citigroup, Inc.*, 2013 WL 3855589, at *6-7 (N.D. Cal. July 24, 2013) (determining that third parties accessing plaintiff's bank account and divulging her contact information did not constitute a serious invasion of a privacy interest); *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (2d Dist. 2011), *as modified* (June 7, 2011) ("obtaining plaintiff's address without his knowledge or permission, and using it to mail him coupons" was "not an egregious breach of social norms, but routine commercial behavior").

Plaintiffs' reliance on *Facebook* is again misplaced. In *Facebook*, the Court held that the plaintiffs had adequately alleged a serious invasion of privacy where they alleged that Facebook acted surreptitiously in *direct contravention* of its privacy disclosures by "correlating users' browsing history with users' *personal Facebook profiles*—profiles that could include a user's employment history and political and religious affiliations," giving Facebook a "cradle-to-grave profile without users' consent." 956 F.3d at 598-99 (emphasis added). Here, by contrast, Plaintiffs (1) consented to Google's receipt of the Data, and (2) do not plausibly allege that Data received by Google while they are logged out and in private browsing mode is correlated with them or their devices after each private browsing session is closed. Without a plausible allegation that Google correlated Data from Plaintiffs' separate private browsing sessions and associated that Data with Plaintiffs, the AC alleges no more than that Google stockpiled information (AC ¶¶ 69, 242). And "merely alleging stockpiling is not enough" to state a privacy claim. *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1042. Plaintiffs' privacy claims should be dismissed.

C. Plaintiffs' Claims Are Barred by the Statutes of Limitations

The statutes of limitations for each of Plaintiffs' claims is either one, two, or three years.[17] Where, as here, the running of the statute of limitations "is apparent on the face of the complaint," a claim may be dismissed pursuant to Rule 12(b)(6). *Hakimi v. Societe Air France, S.A.*, 2018 WL 4826487, at *3 (N.D. Cal. Oct. 4, 2018) (quoting *Jablon v. Dean Witter & Co.*, 614 F.2d 677, 682 (9th Cir. 1980)).

Plaintiffs allege that Google has been intercepting their communications with websites since at least June 1, 2016. AC ¶¶ 11, 192. Yet, they did not file their claims until June 2, 2020—well

[17] *See* 18 U.S.C. § 2520(e) (statute of limitations on Wiretap Claim is "two years after the date upon which the claimant first has a reasonable opportunity to discovery the violation"); *Brodsky*, 445 F. Supp. 3d at 134 ("Under the CIPA, the applicable statute of limitations is one year."); *Lauter v. Anoufrieva*, 2011 WL 13175659, at *7 (C.D. Cal. Nov. 28, 2011), *aff'd*, 550 F. App'x 473 (9th Cir. 2013) ("A claim for invasion of the California constitutional right to privacy has a statute of limitations of one year."); *Guillen v. Bank of America Corp.*, 2011 WL 4071996, at *10 (N.D. Cal. Aug. 31, 2011) (limitations period for intrusion upon seclusion is "one year in California"); Cal. Penal Code § 502(e)(5) (statute of limitations for CCCL is "three years of the date of the act complained of, or the date of the discovery of the damage, whichever is later").

beyond any applicable statute of limitations. Cognizant of this defect, Plaintiffs insist that they "only learned of the truth [about Google's alleged misconduct] in the weeks leading up to the filing of this Complaint," and ask the Court to "toll" the limitations periods on their claims in light of Google's alleged misrepresentations to users regarding private browsing mode. *Id.* ¶ 153, § VII.

But Plaintiffs do not plausibly allege any "fraud" or "misrepresentation" by Google that warrants tolling. The relevant portions of Google's Privacy Policy—of which Plaintiffs received notice and consented—have consistently and expressly disclosed that Google ordinarily receives the Data from Google account holders like Plaintiffs. *See supra* § II.B (citing historic versions). And the Incognito Notice (and Google's other private browsing disclosures) consistently informed Plaintiffs that the practical effects of private browsing are far more limited than Plaintiffs purportedly believed. *See supra* § II.C. Plaintiffs' allegation that Google represented that private browsing would *prevent* Google from receiving the Data is thus rebutted by the very documents on which Plaintiffs rely. Accordingly, there is no basis to apply equitable tolling.

Nor does the delayed-discovery rule apply. Plaintiffs fail to satisfy their burden to "plead specific facts to show … the inability to have made earlier discovery despite reasonable diligence." *Fox v. Ethicon Endo-Surgery, Inc.*, 35 Cal. 4th 797, 808 (2005) (citation and quotation marks omitted); *see also Plumlee v. Pfizer, Inc.*, 2014 WL 695024, at *8 (N.D. Cal. Feb. 21, 2014) (Koh, J.) ("The burden is on the plaintiff to show diligence [warranting application of the discovery rule], and conclusory allegations will not withstand a motion to dismiss."). Google pointed out this defect in its Motion to Dismiss the original Complaint, ECF No. 53 at 20-21, and Plaintiffs fail to cure it.

Plaintiffs offer *no* allegations to meet their burden of establishing diligence—much less reasonable diligence—in attempting to discover Google's alleged misconduct. Indeed, Plaintiffs do not allege that they took even the most basic step of taking Google up on its offer, in the Privacy Policy, to "contact us" "if you have any questions" about Google's practices. *See* Ex. 1 at 1. Plaintiffs' lack of diligence is striking given that their Complaint cites publicly-available articles from 2018 as "evidence" of Google's purported misconduct. *See* AC ¶ 106 (citing Aug. 15, 2018 paper); ¶ 109 (citing Nov. 1, 2018 article). This Court has rejected application of the discovery rule

where, as here, "the Complaint identifies and relies upon several published articles" regarding the allegedly concealed facts "that were published many years before Plaintiff filed suit," and the plaintiff failed to "explain why she was unaware of these publications before … she allegedly discovered the misrepresentation for the first time, nor explain[] why these publications did not serve to put her on notice that Defendant may have made misrepresentations."[18] *Plumlee*, 2014 WL 695024, at *9.

The law is clear that where, as here, "Plaintiff does not allege that she took *any* steps towards discovery," the discovery rule does not apply. *Id.* (emphasis in original). Accordingly, Plaintiffs' claims are barred by the applicable statutes of limitations, and neither tolling nor the discovery rule can save them.

IV. CONCLUSION

For the foregoing reasons, the Court should dismiss this action in its entirety with prejudice.

DATED: October 21, 2020

QUINN EMANUEL URQUHART & SULLIVAN, LLP

By */s/ Andrew H. Schapiro*

Andrew H. Schapiro (admitted *pro hac vice*)
andrewschapiro@quinnemanuel.com
191 N. Wacker Drive, Suite 2700
Chicago, IL 60606
Telephone: (312) 705-7400
Facsimile: (312) 705-7401

[18] Any attempt by Plaintiffs to invoke the continuous accrual doctrine would be misplaced because "California courts have largely confined the application of the continuing accrual theory to a limited category of cases, including installment contracts, leases with periodic rental payments, and other types of periodic contracts that involve no fixed or total payment amount." *Brodsky*, 445 F. Supp. 3d at 136 (citation and quotation marks omitted). "This court has repeatedly noted that when an alleged duty 'bears little relation to the monthly payments or monthly bills that California courts have found to be periodic, recurring obligations,' applying the continuous accrual doctrine is unwarranted." *Id.* at 136-37 (citation omitted). Nor does the continuing violation doctrine apply "to rescue … time-barred claims": "[T]he continuing violation doctrine applies *only* where 'a wrongful course of conduct [becomes] apparent only through the accumulation of a series of harms,'" "but not when a plaintiff experiences 'a series of discrete, independently actionable alleged wrongs.'" *Id.* at 137-38 (quoting *Aryeh v. Canon Bus. Solutions, Inc.*, 55 Cal. 4th 1185, 1199 (Cal. 2013)) (emphasis added).

Stephen A. Broome (CA Bar No. 314605)
stephenbroome@quinnemanuel.com
Viola Trebicka (CA Bar No. 269526)
violatrebicka@quinnemanuel.com
865 S. Figueroa Street, 10th Floor
Los Angeles, CA 90017
Telephone: (213) 443-3000
Facsimile: (213) 443-3100

Diane M. Doolittle (CA Bar No. 142046)
dianedoolittle@quinnemanuel.com
Thao Thai (CA Bar No. 324672)
thaothai@quinnemanuel.com
555 Twin Dolphin Drive, 5th Floor
Redwood Shores, CA 94065
Telephone: (650) 801-5000
Facsimile: (650) 801-5100

William A. Burck (admitted *pro hac vice*)
williamburck@quinnemanuel.com
Josef Ansorge (admitted *pro hac vice*)
josefansorge@quinnemanuel.com
1300 I. Street, N.W., Suite 900
Washington, D.C. 20005
Telephone: 202-538-8000
Facsimile: 202-538-8100

Jonathan Tse (CA Bar No. 305468)
jonathantse@quinnemanuel.com
50 California Street, 22nd Floor
San Francisco, CA 94111
Telephone: (415) 875-6600
Facsimile: (415) 875-6700

Attorneys for Defendant Google LLC